AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

NEW DOMAIN, NEW DIRECTION: Toward a Theory on Cyberspace Control and Use

by
Cory S. Hollon, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Mr. Roger W. Philipsek

Maxwell Air Force Base, Alabama

April 2012

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

This paper addresses the topic of cyberspace theory. Although the explosion in recent years of cyberspace capabilities has resulted in a plethora of examples on how to use the cyberspace domain, no authors have attempted a systematic approach to addressing control and use of the domain from a theoretical perspective. This paper attempts to fill that gap and begin a debate about the best ways to begin to gain control of the domain and then how to exercise that control. After examining both air and naval power theory for useful concepts, this paper attempts to redefine the levels of control possible in cyberspace to differentiate it from the air domain. From there an examination of the use of the domain in obtaining military objectives and a brief look at the nature of cyberwarfare follows. Ultimately, this paper proposes that a more robust examination of the cyberspace power theory will enhance the doctrinal discussions and give the joint force commander more options.

> *"Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur."*[1]
>
> Giulio Douhet

> *"Rapidity of modern means of communication, the sureness of various means of transportation, and the accessibility of all parts of the world to aircraft, which have been developed in an incredibly short space of time, make it absolutely necessary that we organize to meet modern conditions."*[2]
>
> Billy Mitchell

The use of cyberspace to attack and defend U.S. interests is a significant topic because of the pervasiveness, vulnerability, and currency of the domain. Cyberspace has become an ever-present force in the modern, industrialized world. With the advent of smart phones and wireless technology, information is available to people at any time in any place. The pervasiveness of cyberspace has even shown itself in the military where reliance on cyberspace for day-to-day operations is seen in everything from electronic mail as the primary means of communication in garrison to reliance on networked systems in combat.[3] However, most critics of cyberspace also point out the vulnerability of cyberspace to attacks from both state and non-state actors.[4] Additionally, cyber attacks have already been conducted both in the United States and abroad.[5]

A plethora of articles and books exist on how the United States and other countries should respond to these threats; however, there has been little work done on the development of cyberspace theory in the literature. Current cyberspace power theory focuses on either a doctrinal use of cyberspace, what will be termed cyber operations in this paper, or the application of land, sea, and air theory to the domain of cyberspace. Neither approach is wholly satisfying. Doctrine should be informed by an underlying theory lest it become ceaselessly reactive to each new experience in the domain. Additionally, while applying old theoretical frameworks to the new domain has some degree of merit, the radically different nature of cyberspace requires a radically different theory. For example, air dominance has been the norm for so long that it has invaded

every aspect of thinking. Now, even the Secretary of the Air Force has said that we must achieve cyber dominance.[6] However, in the grand scheme of things, the U.S. does not even have air dominance in the worldwide air environment. We have localized air dominance, air supremacy and air superiority depending on the region and the time of day. Because cyberspace operates globally and continuously, it is impossible to envision an environment where U.S. forces have "cyber dominance." Unless those with competing interests are excluded from the cyber domain, there will never be such a thing. Rather, thinking needs to shift to achieving a state where commanders have general freedom of action while allowing for the random attacks. The idea of attempting to achieve cyber dominance leads us down the road of trying to defend everything at all times. Sun Tzu remarked on the folly of this endeavor centuries ago.[7] It is no less a folly today. Cyberspace theory needs to be developed to provide a solid framework for discussion of what is possible in the domain.

The theory, however, will still have to answer two basic topics: how a state gains *control* of cyberspace and how a state *exercises* that control. On an operational level, any theory about the application of force informs doctrinal debate over how the United States can apply that particular force. For example, airpower theory suggests that air superiority is a necessary prerequisite for application of an air force's power. Theories differ on both how to gain control of the air and the manner in which airpower should be utilized to contribute to the achievement of military objectives; however, the theories address one of these two issues. Doctrine, then, explains how to best go about achieving what theory claims needs to be done. This paper intends to address the dearth of cyberpower theory by suggesting a framework for cyberspace theory and contributing to the debate by offering a limited theory about the control of cyberspace.

Stuart H. Starr appeared to address the deficiency in cyberspace theory in his article entitled “Toward a Preliminary Theory of Cyberpower.” He argued that a theory needed to address things like definition of key terms and anticipation of future trends in the field.[8] Unfortunately, his preliminary theory does not address the areas needed for a warfighting theory because his focus is more on the policy implications and capability potential for cyberspace. While this is useful in exploring the topic of cyberpower generally, it does little to advance an understanding of how military forces should view the domain. Instead, a military theory on cyberspace use should address the traditional subjects of control of the domain and use of that control in order to lay a better foundation for doctrinal development.

Cyberspace is one of the more vulnerable centers of gravity for a technologically advanced country like the United States. Matters of time and distance are not applicable to cyberspace because of the nature of the domain. Any state or non-state actor can bring the full force of his cyberpower to bear on any other actor. Control of cyberspace must be a priority, but the level of control will be lower than United States forces are accustomed in domains like the air. A relative advantage in cyberspace is what operators should be seeking to achieve.

Relative advantage in cyberspace, encapsulated in the term *cyber preeminence* should mean a relative freedom from and to attack along with the ability to rapidly recover from any attack on the computer network. Complete dominion over cyberspace is unrealistic because of the relative ease of entry into the domain and inappropriate because the use of cyberspace by civilian actors should not be under the scrutiny or control of the military. The historical analogy between the emergence of cyberpower now and the emergence of airpower in the inter-war years is accurate. As such, the concept of cyber preeminence could mirror the concept of air superiority as it was applied in WWII. When General Pete Quesada was accused of not providing

air superiority over France, he investigated the allegation and retorted that air superiority meant relative freedom of movement, not the absence of any attacking force. This is the same understanding cyberspace forces should take today in regards to control of cyberspace. Relative freedom of operation in cyberspace does not mean that computer networks will never be attacked or that information will never be compromised. It should mean, however, that *on balance* the adversary has less ability to exploit the domain than friendly forces do.

Before providing a framework for cyberspace theory, though, two tasks need to be completed. First, cyberspace must be defined. Science-fiction author William Gibson coined the term cyberspace in 1982 in a short story published in Omni Magazine.[9] The Oxford English Dictionary defines cyberspace as "the notional environment within which electronic communication occurs, esp. when represented as the inside of a computer system."[10] This definition has its limits when trying to understand cyberspace as a war-fighting domain because it narrows cyberspace to only that area where communication takes place. The Merriam-Webster dictionary narrows the definition even further by defining cyberspace as "the online world of the Internet."[11] While this conveys the popular understanding of what cyberspace is, it also limits it to only the internet. In May of 2009, the Department of Defense sought to remedy the problem of definition by issuing guidance on what cyberspace is. Only three years before had the *National Military Strategy for Cyber Operations* labeled cyberspace as a domain on par with land, sea, air, and space.[12] By defining cyberspace as a domain, the Department of Defense (DoD) delineated the physical aspects of cyberspace and limited how humans can act in it. Cyberspace is "the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[13] Within these networks, humans use electrons to act; however, the military effects created there

are completely dependent on how the humans decide to use electrons within the domain.[14] Because this definition specifically addresses the infrastructure of cyberspace and allows for military effects to be achieved within this space, the DoD definition will be used for this paper.

Second, it must be understood what the previous theories have to offer cyberspace in terms of structure and inspiration for understanding a new cyberspace theory. Previous theories concerning naval and airpower are most appropriate as they discuss the two areas germane to a theory: control of the domain and use of the domain. Most often, airpower theory is used as the basis for discussion of cyberspace operations because the United States Air Force, as an institution that owed its existence to technology, was an early adopter of new technology and has the preponderance of cyber forces in the U.S. military.[15]

Early airpower advocates Billy Mitchell and Giulio Douhet both discussed how to gain control of the air domain and how to use that control. Both these theorists understood control of the air to mean having the freedom to use the domain without significant interference from the enemy.[16] Douhet claimed that "to have command of the air means to be in a position to prevent the enemy from flying while retaining the ability to fly oneself."[17] Further he argued that "in order to conquer the air, it is necessary to deprive the enemy of all means of flying, by striking at him in the air, at his bases of operation, or at his production centers – in short, wherever those means are to be found."[18] Douhet argued for what we would understand as air supremacy, which is the complete domination of the air domain. Mitchell argued that "aviation must attack to bring results. It cannot dig trenches or dugouts in the air and assume the defensive. It must go after its adversary, wherever he is, and either destroy him or be destroyed. There is no middle course."[19] In other words, airpower is inherently offensive. The principle aim of an air force was to gain and maintain air superiority. For Mitchell, that meant the destruction of the enemies' air force.[20]

His experience in World War I convinced Mitchell that air battles must be won in order to establish control of the air.[21] He also felt that the only defense against the airplane was other airplanes. “Once airplanes have beaten the hostile aircraft in air battles, nothing can stop their operations.”[22] In contrast to Mitchell, Douhet believed that bombing air forces on the ground would be the surest way of gaining command of the air domain.[23]

Current USAF doctrine does not delineate between air superiority and air supremacy, but NATO doctrine does give insight into what is required to achieve these levels of control. USAF doctrine defines air superiority as “that degree of dominance in the air and space battle of one force over another which permits the conduct of operations by the former and its related land, sea, air and space forces at a given time and place without prohibitive interference by the opposing force.”[24] NATO introduces the concept of air supremacy as “the degree of air superiority wherein the opposing air force is incapable of effective interference.”[25] A third possibility exists; however, this is not addressed in official USAF or NATO doctrine. If neither side has clearly established air superiority, then a state of air parity is present. These concepts are well established and stem from the initial writings of Mitchell and Douhet.

In addition to their disagreement about the best way to gain control of the air, Mitchell and Douhet also disagreed about the best way to use that control. Douhet held that bombing the enemy’s population centers to destroy the will of the people to continue to fight was the best use of command of the air.[26] Mitchell held that air power could make wars less grisly than WWI because it had the ability to strike directly at the heart of the enemy. “The air forces will strike immediately at the enemy’s manufacturing and food centers, railways, bridges, canals and harbors.”[27] Instead of directly targeting the population, Mitchell wanted to attack the industry that supported the enemy’s ability to make war.[28] Airpower made it possible to do this quickly

and relatively cheaply. “Aircraft operating in the heart of an enemy’s country will accomplish this object in an incredibly short space of time . . . and the months and even years of contest of ground armies with a loss of millions of lives will be eliminated in the future.”[29] Ultimately, Mitchell and Douhet believed that military objectives could be accomplished more quickly through the application of power directly at the heart of the enemy through the air domain.

While cyberspace theorists have most often turned to airpower theory for concepts and understanding of the domain, naval theory holds more promise because of the similarities between the sea and cyberspace in terms of potential for control and use of the domain without absolute control of it. British naval historian Julian Corbett argued that the object of naval warfare was to ensure that a nation had a superior naval force that guaranteed command of the sea.[30] For Corbett, “the only positive value which the high seas have for national life is as a means of communication.”[31] Command of the sea means the ability to control that communication.[32] There are two parts to command of the sea: gaining command and exercising command.

Gaining command of the sea necessitates the destruction of the enemy’s naval force. Any action that is directly focused on the enemy’s fleet is considered to be an action toward gaining control of the sea. Corbett offers two approaches to accomplish this objective: decisive battle and blockade.[33] Both of these methods aim at decreasing the amount of force an enemy can bring into action. While he often argues against seeking out the enemy fleet for practical reasons, gaining command of the sea “can only be obtained permanently by the destruction of the enemy’s armed forces afloat.”[34] Permanent naval superiority, like air superiority, requires the eradication of the opposing naval power; however, Corbett notes that a country can never achieve this state in practice.[35] Corbett asserts that “a Power [sic] too weak to win command by

offensive operations may yet succeed in holding the command in dispute by assuming a general defensive attitude."[36]An enemy force capable of any kind of activity can still contest for command of the sea by striking at the opposing naval power. Therefore, control of the sea can never be fully realized, but exercising command of the sea can happen simultaneously with the efforts to gain command.

Corbett fundamentally differs from air theorists by positing a method to employ naval power without having full naval superiority. Exercising command of the sea is using the sea lines of communication for friendly purposes or interfering with the enemy's use of them.[37] In exercising command, naval forces further limit what the enemy can bring to bear by acting against anything attempting to use the sea as a line of communication.[38] Corbett argues that "naval warfare does not begin and end with the destruction of the enemy's battle fleet . . . there is the actual work of preventing his passing an army across the sea and of protecting the passage of our own."[39] He maintains that there are three methods of exercising command: defending against an invasion, attacking or defending commerce, and supporting military operations. The goal of naval warfare then is to use command of the sea in order to affect either the military objectives or exert pressure on commerce.

Cyber theory has generally been discussed in terms of previous air theory, but naval theory has a more satisfactory application. In terms of control of the domain, airpower theory demands a level of control that is not possible in the cyber realm. Air Force Secretary Michael Wynne called for superiority in cyberspace and concluded "cyber superiority is the prerequisite to effective operations across all strategic and operational domains."[40] This hearkens back to Mitchell and Douhet claiming that air superiority was the necessary precursor to all military operations. Unfortunately, because of the relative ease of entry into the cyberspace domain and

the inability to adequately prevent an adversary from using cyberspace completely, the concept of air superiority as understood by Mitchell and Douhet is of dubious merit to the current debate. Both of these thinkers applied their talents to a domain that could be effectively closed off to an enemy nation and was beyond the economic reach of non-state actors. The demand to obtain superiority or even dominance in the cyberspace domain is a misapplication of airpower theory to a realm that is significantly different. Julian Corbett's understanding of control of the sea, however, is much more promising because of his recognition that a "force in being" could always contest generalized command of the sea and that preventing access to the sea could be as useful as destroying the opposing forces entirely. Ultimately, Corbett's naval theory is a better interpretative lens through which to view cyberspace because of the nature of the domain.

Cyberpower theory can take lessons from both airpower and naval theory in considering the use of the domain; however, the general dividing line between gaining control and exercising control should come from naval theory. Corbett understood that operations to exercise command of the sea could occur before, during, or completely independently of operations to gain command. Airpower has a similar concept called "localized air superiority," which means that air forces have freedom of action within a constrained geographical space and only for a specified amount of time. Uncontested control of cyberspace should be understood as a localized event which will probably only be present for very small amounts of time; however, the effects that can be achieved through cyber are both more important than and independent from gaining this type of control.

The issue now becomes the meaning of cyberspace control and the best method of exercising that control. Generalized control of cyberspace is, like command of the sea, an unrealistic goal. Instead, cyberspace requires a different understanding for control of the domain. Unfortunately,

because Airmen have been the primary participants in the debate about cyberspace, airpower theory terms have been misapplied to the subject. However, in addition to the reasons stated above, airpower theory does not allow for the transient nature of cyberspace control where attacks can happen in milliseconds and without warning. Dominance in a theater, especially for airpower, has become the norm for U.S. forces after the first few days of major combat operations. This will not be the case for cyberspace. Instead, operators will need to address what level of control is required for operations.

The key phrase to take away from the doctrinal definition of air superiority is "without prohibitive interference from the opposing force;" however, air supremacy, as understood from NATO doctrine, in a theater after the first few days of major combat operations has become the norm. This has resulted in skewed thinking about the true definition of what air superiority is. The traditional understandings of air superiority and air supremacy are not truly applicable to cyberspace. Instead, as a new domain, cyberspace should have an entirely new vocabulary when discussing the control of that domain.

Developing new terms for control of cyberspace will result in several advantages. First, this will allow theorists to cast off the connotations of doctrinal terms associated with other domains. This should allow them to avoid misapplying old theoretical frameworks to the new domain. Second, as thinkers and operators develop the tools to implement control of the domain, the new terms will allow for more flexibility in their meaning. Third, new terms and, thus, new meanings, will more accurately represent what is possible in the domain of cyberspace. If the operators have a new set of terms from which to work, the connotations and doctrinal refinement can more closely represent the realities of cyberspace as opposed to the thin-slicing that often takes place when attempting to apply old paradigms to new situations. Finally, the new vocabulary will also

allow commanders to give more detailed guidance on the amount of control required for a given operation thus allowing their planners and operators to appropriately focus their efforts on the effects required for the force.

The first term suggested is *cyber ascendancy*. This is to be defined as the generally unachievable state of complete control over both friendly and adversary cyberspace power. It would only be achievable if the opposing force had no cyber capability because of either direct action or a completely undeveloped cyber capability. For example, if the United States were to go to war with Liberia, which has approximately 0.5% of its population with internet access, cyber forces could claim that the United States had achieved cyber ascendancy in that country.[41] Similarly, if a military had destroyed or blocked all electronic communication lines in a country, it would have achieved cyber ascendancy. However, if the opposing country had access to the internet for communications or could launch attacks against the adversary's network, then cyber ascendancy would not be present.

The second term suggested is *cyber preeminence* and it is most likely the highest level of control realistically achievable in real operations. It means a relative advantage in using cyberspace for friendly purposes and the ability to recover from attacks quickly. Preeminence is most analogous to air superiority in that it assumes relative freedom of maneuver in the cyber realm and limiting the impact of an adversary's attacks.[42] This does not imply that computer networks will never be attacked, but it does require that recovery from those attacks is swift and complete. For example, assume country A has a cyberspace system that allowed them storage of classified data and use of an internet system for command and control. Country A could be said to have cyber preeminence if they could detect and stop attacks on that system before experiencing critical loss in either capability or data. If country B could hack into the system but

only shut it down for a few minutes or hours, the case could be made that preeminence was still present, but at a lower degree. Ultimately, if one party to a conflict can use cyberspace as they wish without unrecoverable damage to the system as a result of the adversary's actions, then they have achieved cyber preeminence.

If, however, neither side can claim freedom of maneuver or the ability to recover quickly from attacks, be that because of the enemy's persistence in attack or a critical failure in the infrastructure, then the condition should be called *cyber equality*. This is comparable to concept of air parity where neither side has a marked advantage of the other. Cyber equality, like cyber ascendancy, is rare because most countries have taken action to either restrict access to their critical networks or prepare for restoration of services in the event of an attack.

The key in obtaining cyber preeminence is the ability to recover quickly from an attack because "the irrelevance of distance and the speed of cyber operations already make it clear that the advantage in cyberspace goes almost entirely to the offense."[43] In order to do this, cyber forces need to concentrate on survivability, redundancy, integration, location, and vulnerability. Cyberspace is more than just the physical infrastructure of wires and computers. It is also the links between space-based assets and controlling ground stations. These links can be attacked via kinetic means and can be stolen or altered with relatively inexpensive equipment.[44] In order to be survivable, both the physical structures and the wireless links need protection in the form of either active defenses or signal shielding to prevent their corruption and denial.

Additionally, military forces should be able to project cyberspace power through a variety of channels. As mentioned before, this means not relying solely on space-based enablers or wireless communications. Gaining preeminence in cyberspace requires providing redundancy to these

methods with fiber optic cable.[45] If an adversary has denied or compromised one avenue of cyberspace action, it should not completely preclude a friendly force from using cyberspace.

Similar to redundancy, integration of the multiple avenues for utilization of cyberspace is a key to its recoverability. If cyber access from one point or system is denied or degraded, for example, an integrated system can be used to fill in the gaps in coverage or share the workload. Recent successes in feeding information from ground based terminals in Southwest Asia to sites in Germany in order to capitalize on satellite bandwidth demonstrates the United States Air Force's (USAF) competency in integrating scarce resources already.[46] Further integration will only increase the ability of cyber operators to utilize scarce resources in efficient and effective ways. In addition, the United States' asymmetric airpower advantage could be integrated to achieve cyber effects. For example, if the adversary had two means of communicating with the front lines, a kinetic attack could eliminate one of those means while cyber exploitation could be used to gain information from the other. In this example, the kinetic attack would be considered part of gaining control of the domain and, thus, contributing to cyber preeminence; the exploitation would be a use of the cyber domain.

Next, locating networks in an intelligent way can lead to quicker recovery from an attack. For example, the RIPRnet (Radio Over Internet Protocol Routed Network), an IP network developed to extend line of sight communications in the Iraq theater, could place communication networks on top of an internet router network. While still heeding the need for redundancy, this type of layering could preempt the need for airborne relays and result in greater efficiency in the cyber realm.[47]

Finally, if an attack can be prevented, the need for recovery is rendered moot. That is why the final task for cyber operators is decreasing the vulnerability of networks. Cyber attackers

introduce worms, viruses, and phishing programs in addition to other types of malware through software. Hardware can also include risks, which is one of the reasons the USAF banned thumbdrives in 2010.[48] Education of users can help prevent some of these attacks, but the cyber acquisition field needs to consider inherent vulnerabilities when contracting for hardware and software. It would be unthinkable for a service to use combat technologies produced in a foreign country when there was no way of determining if there was a critical deficiency or potential for adversary access being present; however, current DoD software and hardware are manufactured overseas and may contain malicious code undetectable by current scans. To effectively establish cyber preeminence, this vulnerability must be addressed.[49]

The amount of cyber preeminence needed by a combatant commander will depend on the type of operation being conducted. In a counterinsurgency fight, more control will be needed over information in order to thwart the insurgency, but the freedom to attack will not be as important because of the asymmetry inherent in the conflict. In a limited conventional war, cyber preeminence is necessary in order to be able to stay inside the decision making loop of the adversary; moreover, a higher degree of cyber preeminence is desired because of the freedom from attack it would allow. Decisions about the amount and targets of cyber attack would need to be made in consultation with the national or theater command authority because of the possibility of escalation. In an unlimited conventional war, a small level of cyber preeminence is all that can be realistically expected because of the number of other operations that are going on. Emphasis should be placed on defense of computer networks and rapid recovery from network attacks.

Even without control of the domain, cyberspace can still be used to achieve military effects. For example, consider an airplane that can travel near the speed of light and completely undetected by enemy observation mechanisms. Even if a country has a fully functioning and

highly advanced integrated air defense system, the airplane could hold any target in the country at risk. Such a weapon would render traditional claims of air supremacy moot because it could completely bypass the defenses. The enemy's control of the domain would not be challenged, but airpower would be used in a way that was advantageous for the opposing force. Cyberspace has this ability. Therefore, it is necessary when discussing a cyberspace theory to examine some possible uses of cyberspace that do not directly relate to gaining any degree of domain control.

Like exercising command of the sea to affect the lines of communication for a country, using cyberspace can have effects on both military and civilian targets. John Boyd claimed that the key to winning a conflict was being more efficient and effective at orientation to the circumstances at hand.[50] New information is critical to effectively orientating decision makers to the actual situation.[51] Modern militaries are dependent on cyberspace for communication, control, intelligence, surveillance, and reconnaissance in addition to storing information gathered. Cyberspace can act directly against this line of communication by either delaying or denying information critical to the adversary's decision-making process. Because cyberspace offers a link from the physical world to the mental world of the adversary leadership, "then it follows that cyberspace operations offer unprecedented promise for shaping the battlespace and affecting the perceptions and actions of the adversary."[52] Additionally, effective orientation benefits from knowing what information the adversary has accessed. Cyberspace exploitation can then aid the commander in developing a more accurate mental picture of the battlespace and deny the same to his adversary.

Cyber attacks against civilian networks are another example of how cyber can be used to coerce an adversary to act in a certain way. Against an adversary who is highly dependent on cyberspace, cyber can affect power grids, oil and gas pipelines, chemical refineries, and even

financial and banking systems.[53] Further, cyber can couple with traditional strategic communications methods to influence the will of the adversary both at the popular and national command levels.[54] Major Leland Bohannon gives an excellent discussion of the myriad of ways that cyber can be used both before and during open hostilities; his work will not be repeated here except to caution against drawing to strong of a conclusion about the ability of cyber.[55] In discussing preemptive cyberspace attacks, Major Bohannon argues that "cyber operations can be more persuasive than mere diplomacy while remaining less costly than combat."[56] This could be construed as promoting cyberspace, like Mitchell and Douhet promoted airpower, as being able to win a conflict alone. While Major Bohannon makes no such radical claim, it must be cautioned against leading down that path as it misrepresents the capabilities and overlooks the limitations of cyberspace operations.

When deciding to use cyberspace, though, national leaders and commanders must understand the potential implications these actions may have. Because cyberspace, by definition, does not have international boundaries, there are some concerns over what would constitute an act of war in cyberspace. In 2007, for example, Estonia's networks were attacked by denial of service and hacking techniques in combination with violent protests in response to their decision to move a statue commemorating the Soviet Union's liberation of the country during WWII. The attacks could not be conclusively traced to Russia, but Estonia believed that both the protests and the cyber attacks both originated from there.[57] Estonia did not respond militarily, but the question remains as to whether or not they would have been justified to do so. Because of difficulties in attribution, it is difficult to predict what a country may do in response to a cyber attack especially one that targeted civilian infrastructure.

Additionally, cyber war is more likely to be an unlimited war because of the nature of the domain. All the resources of a country in cyberspace can be brought to bear in the conflict with limited delay. As Corbett cautioned, limited war is only possible "between Powers which are separated by sea, and then only when the Power desiring limited war is able to command the sea to such a degree as to be able not only to isolate the distant object, but also to render impossible the invasion of his home territory."[58] Because cyberspace is an interconnected network, countries that decide to attack face the possibility of an escalated, total cyber war.

Cyber power is inherently an offensive weapon. The limited ability of computer network defense operations to completely secure a network mean that cyberpower, like airpower, should be used primarily as an offensive weapon. However, the theories governing cyberpower employment have misapplied airpower theoretical concepts. Instead, naval theory should be used in conjunction with a new vocabulary to allow cyberspace power to develop and meet the challenges of its domain. As the world becomes more interconnected, cyberspace control and use will become more important to military and civilian leaders alike. Only with the proper theoretical framework can military forces help to realize the full extent of cyberpower's contribution to the national defense.

BIBLIOGRAPHY

"Air Force's Banning of Thumb Drives Temporary Solution to WikiLeaks." http://www.infosecurity-magazine.com/view/14762/air-forces-banning-of-thumb-drives-temporary-solution-to-wikileaks/. 17 December 2010. Accessed 17 March 2012.

Air Force Doctrine Document 1-2. *Air Force Glossary*, 11 January 2007.

Blank, Stephen. "Web War I: Is Europe's First Information War a New Kind of War." *Comparative Strategy* 27 (2008): 227-247.

Bohannon, Leland. "Cyberspace and the New Age of Influence." Master's Thesis, School of Advanced Air and Space Studies, 2008.

Bosker, A.J. "SECAF: Dominance in Cyberspace is not Optional." http://www.offutt.af.mil/news/story.asp?id=123055205, accessed 20 Nov 2011.

Boyd, John, R., *The Essence of Winning and Losing*, 28 June 1995, http://www.danford.net/boyd/essencex.htm, accessed 18 March 2012.

Convertino, Sebastian M. Lou Anne DeMattei, and Tammy M. Knierim. *Flying and Fighting in Cyberspace*. Maxwell AFB, AL: Air University Press, 2007.

Corbett, Julian. *Principles of Maritime Strategy*. Mineola, NY: Dover Publications, Inc., 2004.

Douhet, Giulio. *The Command of the Air*. Translated by Dino Ferrari. New York, NY: Cowar-McCann, 1942.

Fadok, David S. "John Boyd and John Warden: Airpower's Quest for Strategic Paralysis." In *The Paths of Heaven: The Evolution of Airpower Theory*. Edited by Col. Phillip S. Meilinger. Maxwell AFB, AL: Air University Press, 1997.

Farmer, David B. "Do the Principles of War Apply to Cyber War?" Master's thesis, School of Advanced Military Studies, 2010.

Gibson, William. "Burning Chrome." *Omni Magazine*, July 1982, 72-77.

Grant, Rebecca. *Victory in Cyberspace*. Air Force Association Special Report. Arlington, VA: Air Force Association, 2007.

Internet World Stats: Usage and Population Statistics, http://www.internetworldstats.com/stats1.htm, accessed 15 March 2012.

Jones, Johnny R. *William "Billy" Mitchell's Air Power*. Maxwell AFB, AL: Airpower Research Institute College of Aerospace Doctrine, Research, and Education, September 1997.

Kohn, Richard H. and Joseph P. Harahan, "Editor's Introduction." In The *Command of the Air*. Translated by Dino Ferrari. New York, NY: Cowar-McCann, 1942.

Lambeth, Benjamin S. "Airpower, Spacepower, and Cyberpower." *Joint Forces Quarterly* 60, no. 1 (Spring 2011): 46-53.

Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power Economic and Military.* New York, NY: G.P. Putnam's Son's, 1925.

North Atlantic Treaty Organization Standardization Agency (NSA), *AAP-6 NATO Glossary of Terms and Definitions*, 2008.

Rushe, Dominic. "Cyber-attack Claims at US Water Facility." *The Guardian*, 20 November 2011. http://www.guardian.co.uk/world/2011/nov/20/cyber-attack-us-water-utility?newsfeed=true, accessed 20 Nov 2011.

Simmons, Travolis A. "Operationalizing Cyberspace for Today's Combat Air Force." Master's Thesis, Air Command and Staff College, 2010.

Stallone, Martin. "Don't Forget the Cyber!: Why the Joint Force Commander Must Integrate Cyber Operations Across other War Fighting Domains, and how a Joint Forces Cyberspace Component Commander Will Help." Master's thesis, Naval War College, 2009.

Starr, Stuart H. "Toward a Preliminary Theory of Cyberpower." In *Cyberpower and National Security* edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 43-90. Dulles, VA: Potomac Book, Inc., 2009

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, 16 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, accessed 20 November 2011.

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. Oxford, GBR: Oxford University Press, 1963.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations.* Washington DC: CJCS, September 2006.

U.S. Deputy Secretary of Defense. *The Definition of "Cyberspace."* Policy Dated 12 May 2009.

Wynne, Michael W. "Flying and Fighting in Cyberspace." *Air and Space Power Journal*, Spring 2007.

[1] Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (New York, NY: Cowar-McCann, 1942), 30.
[2] William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power Economic and Military* (New York, NY: G.P. Putnam's Son's, 1925), xv.
[3] David B. Farmer, "Do the Principles of War Apply to Cyber War?" (Master's thesis, School of Advanced Military Studies, 2010), 3-4.
[4] A.J. Bosker, "SECAF: Dominance in Cyberspace is not Optional," http://www.offutt.af.mil/news/story.asp?id=123055205, accessed 20 Nov 2011.
[5] Dominic Rushe, "Cyber-attack claims at US water facility," *The Guardian*, 20 November 2011, http://www.guardian.co.uk/world/2011/nov/20/cyber-attack-us-water-utility?newsfeed=true, accessed 20 Nov 2011. Also, Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, 16 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, accessed 20 November 2011.
[6] Bosker, "SECAF: Dominance"
[7] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford, GBR: Oxford University Press, 1963), 98.
[8] Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Book, Inc., 2009), 44.
[9] *Oxford English Dictionary*, s.v. "cyberspace." This is the source for the information given. For the article referenced in the dictionary entry, see William Gibson, "Burning Chrome," *Omni Magazine*, July 1982, 72-77.
[10] Ibid.
[11] *Merriam-Webster Dictionary*, s.v. "cyberspace."
[12] U.S. Office of the Chairman of the Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (Washington DC: CJCS, September 2006), ix.
[13] U.S. Deputy Secretary of Defense. *The Definition of "Cyberspace."* Policy Dated 12 May 2009.
[14] Martin Stallone, "Don't Forget the Cyber!: Why the Joint Force Commander Must Integrate Cyber Operations Across other War Fighting Domains, and how a Joint Forces Cyberspace Component Commander Will Help" (master's thesis, Naval War College, 2009), 4.
[15] Rebecca Grant, *Victory in Cyberspace*, Air Force Association Special Report (Arlington, VA: Air Force Association, 2007), 18-20. Also, Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower," *Joint Forces Quarterly* 60, no. 1 (Spring 2011): 53.
[16] Douhet, *The Command of the Air*, 24. Also, Alfred F. Hurley, *Billy Mitchell: Crusader for Air Power* (Bloomington, IN: Indiana University Press, 1964), 24-25.
[17] Douhet, *The Command of the Air*, 24.
[18] Ibid., 28.
[19] Johnny R. Jones, *William "Billy" Mitchell's Air Power* (Maxwell AFB, AL: Airpower Research Institute College of Aerospace Doctrine, Research, and Education, September 1997), 9.
[20] Ibid., 27
[21] Mitchell, *Winged Defense*, 199.
[22] Ibid., 203.
[23] Douhet, *The Command of the Air*, 53-54.
[24] Air Force Doctrine Document 1-2. *Air Force Glossary*, 11 January 2007. 40.

[25] North Atlantic Treaty Organization Standardization Agency (NSA), *AAP-6 NATO Glossary of Terms and Definitions*, 2008. 2-A-11.
[26] Richard H. Kohn and Joseph P. Harahan, eds. in Douhet. "Editor's Introduction," viii.
[27] Mitchell, *Winged Defense*, xvi.
[28] Ibid. 126-7.
[29] Ibid, 127.
[30] Julian S. Corbett, *Principles of Maritime Strategy* (Mineola, NY: Dover Publications, 2004), 90.
[31] Ibid., 89.
[32] Ibid., 90. Also, 102.
[33] Ibid., 167.
[34] Ibid., 236.
[35] Ibid., 102.
[36] Ibid., 211.
[37] Ibid., 235.
[38] Ibid.
[39] Ibid.
[40] Michael W. Wynne, "Flying and Fighting in Cyberspace," *Air and Space Power Journal*, Spring 2007, 8.
[41] Internet World Stats: Usage and Population Statistics, http://www.internetworldstats.com/stats1.htm, accessed 15 March 2012. Internet usage is not the best tool for determining the cyberspace capability of a government; however, it is useful in demonstrating the overall connectivity of a particular state and the amount the Internet has penetrated the society.
[42] See Farmer, "Do the Principles of War Apply?" This monograph analyzes the principles of war as applied to the cyber domain and includes a discussion on maneuver in the cyber realm (37-39.
[43] Sebastian M. Convertino, Lou Anne DeMattei, and Tammy M. Knierim, *Flying and Fighting in Cyberspace* (Maxwell AFB, AL: Air University Press, 2007), 71.
[44] Grant, *Victory in Cyberspace*, 24.
[45] Ibid., *24.*
[46] Ibid.
[47] Ibid.
[48] "Air Force's Banning of Thumb Drives Temporary Solution to WikiLeaks," http://www.infosecurity-magazine.com/view/14762/air-forces-banning-of-thumb-drives-temporary-solution-to-wikileaks/, 17 December 2010, accessed 17 March 2012.
[49] Travolis A. Simmons, "Operationalizing Cyberspace for Today's Combat Air Force" (Master's Thesis, Air Command and Staff College, 2010), 9
[50] David S. Fadok, "John Boyd and John Warden: Airpower's Quest for Strategic Paralysis," in *The Paths of Heaven: The Evolution of Airpower Theory*, ed. Col. Phillip S. Meilinger (Maxwell AFB, AL: Air University Press, 1997), 366.
[51] Boyd, John, R., *The Essence of Winning and Losing*, 28 June 1995, http://www.danford.net/boyd/essencex.htm, accessed 18 March 2012.
[52] Ibid., 15.

[53] Leland Bohannon, "Cyberspace and the New Age of Influence" (Master's Thesis, School of Advanced Air and Space Studies, 2008), 77.
[54] Ibid., 78.
[55] Ibid.
[56] Ibid., 17.
[57] Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War," *Comparative Strategy* 27 (2008): 227-228. (227-247)
[58] Corbett, *Principles*, 54.